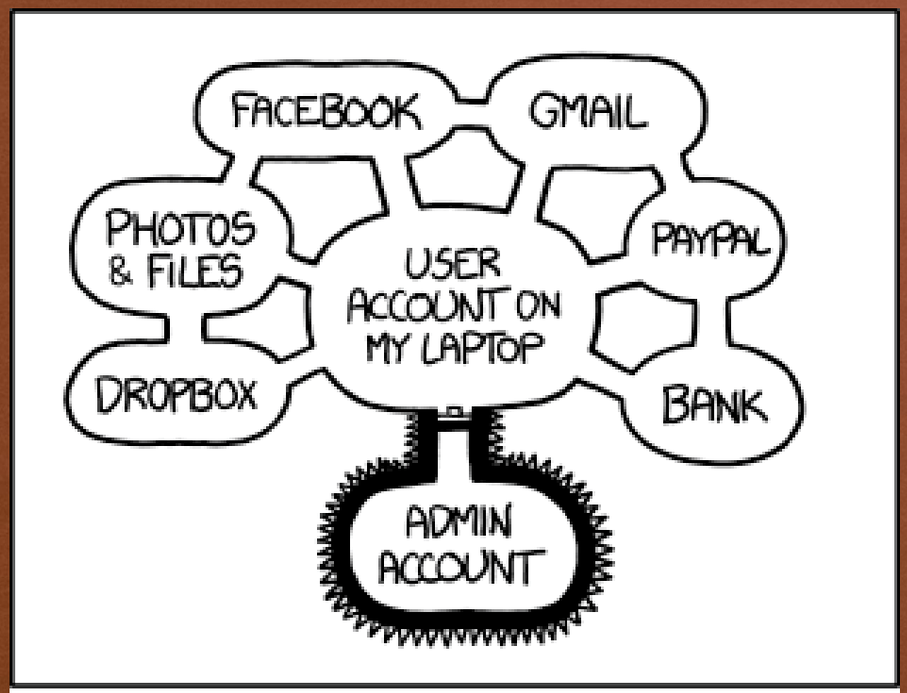
SECURITY

Chapter 8



IF SOMEONE STEALS MY LAPTOP WHILE I'M LOGGED IN, THEY CAN READ MY EMAIL, TAKE MY MONEY, AND IMPERSONATE ME TO MY FRIENDS,

BUT AT LEAST THEY CAN'T INSTALL DRIVERS WITHOUT MY PERMISSION.

https://xkcd.com/1200/

Recap: ENCRYPTION

Types of Cryptographic systems – based on how the plaintext is processed

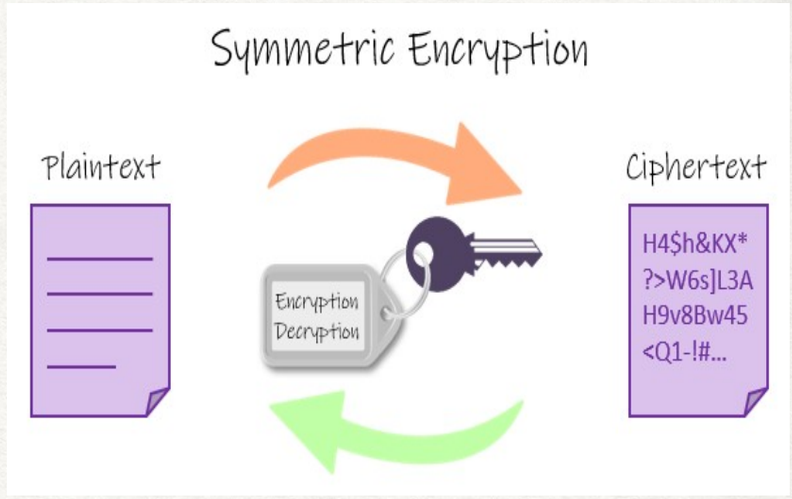
- **Block cipher**
  - processes the input one block at a time, producing an output block for each input block.

- **Stream cipher**
  - processes the input elements continuously, producing output one element at a time, as it goes along.

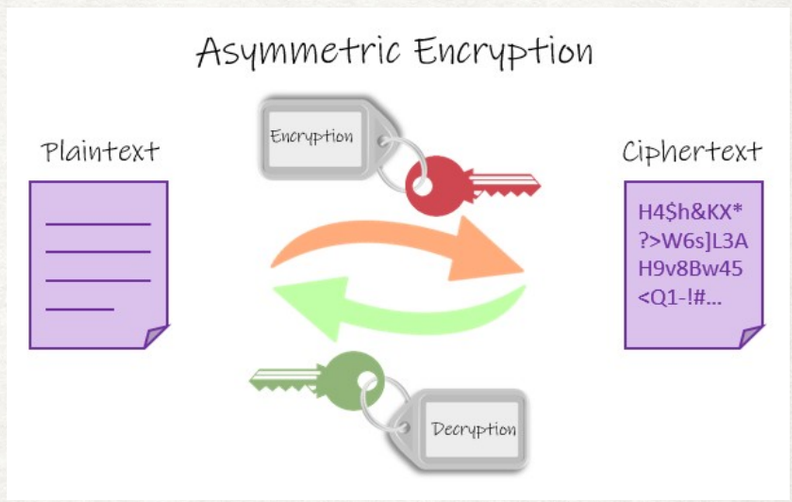
Recap: ENCRYPTION

Types of Cryptographic systems – based on the number of keys used.

- **Symmetric encryption algorithm**
  - A secret key shared by the sender and the receiver
  - Same key is used to encrypt and decrypt
  - Challenge – to securely transmit the secret key



- **Asymmetric encryption algorithm (public key encryption)**
  - Uses two keys: public and private
  - Use public key (generally known) to encrypt
  - Use private key (known only to receiver) to decrypt



SYMMETRIC ENCRYPTION

Three most important and widely used **symmetric block ciphers**:

1. Data Encryption Standard (DES)
2. Triple DES (3DES)
3. Advanced Encryption Standard (AES).

Data Encryption Standard (DES)

- Symmetric encryption algorithm

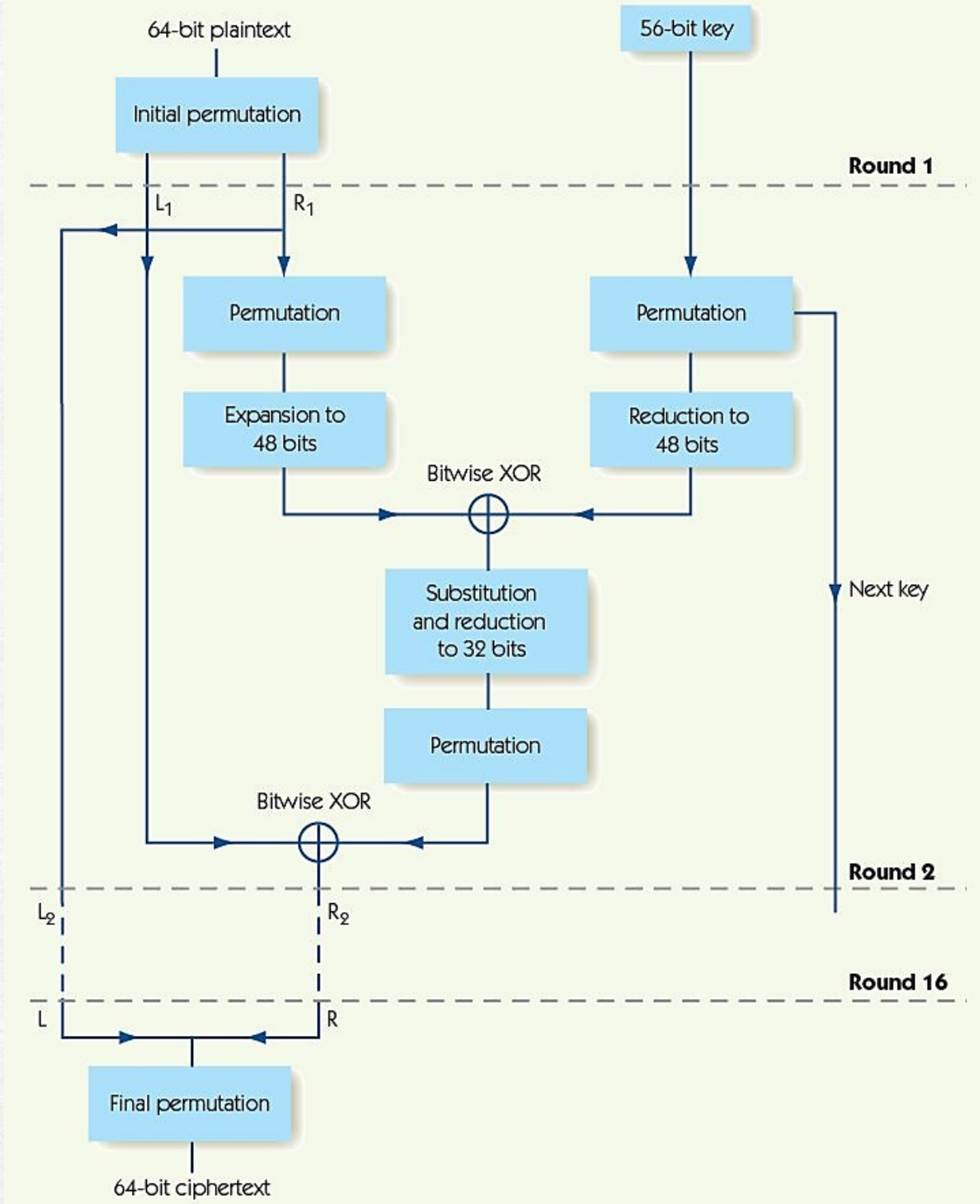
- Designed for digital data; plaintext (64 bit) is a binary string
- Uses 64-bit binary key (56 bits actually used, remaining bits used for error checking)
- Sixteen rounds of the same series of manipulations
- Decryption uses the same algorithm; keys in reverse

- Fast and effective but requires shared key
  - 56 bits is too small for modern technology

Data Encryption Standard (DES)

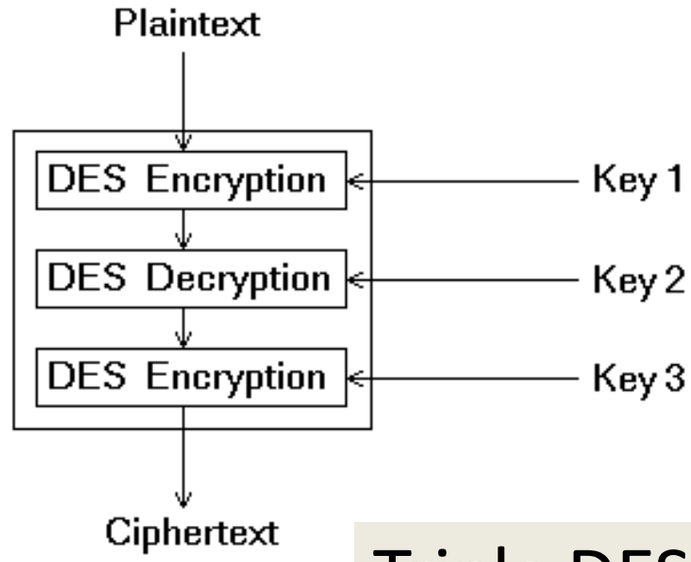
- The plaintext is 64 bits in length
  - longer plaintext amounts are processed in 64-bit blocks
- The key is 56 bits in length;
- There are 16 rounds of processing.
  - From the original 56-bit key, 16 subkeys are generated, one of which is used for each round.
- Decryption uses the same algorithm; keys in reverse.
  - use K16 on the first iteration, K15 on the second iteration & so on.

FIGURE 8.3



The DES encryption algorithm

SYMMETRIC ENCRYPTION



Triple DES

Three most important and widely used **symmetric block ciphers**:

1. **Data Encryption Standard (DES)**
2. **Triple DES (3DES)** - Triple DES improves the security of DES; it requires three 56-bit keys (which can be thought of as a 168-bit key length) and runs the DES algorithm three times; block size 64 bits.
3. **Advanced Encryption Standard (AES)** - uses a similar approach (successive rounds of computations that mix up the data and the key)
   - longer keys (128, 192 or 256 bits)
   - block size (128 bits)

CHALLENGE – SECRET KEY DISTRIBUTION

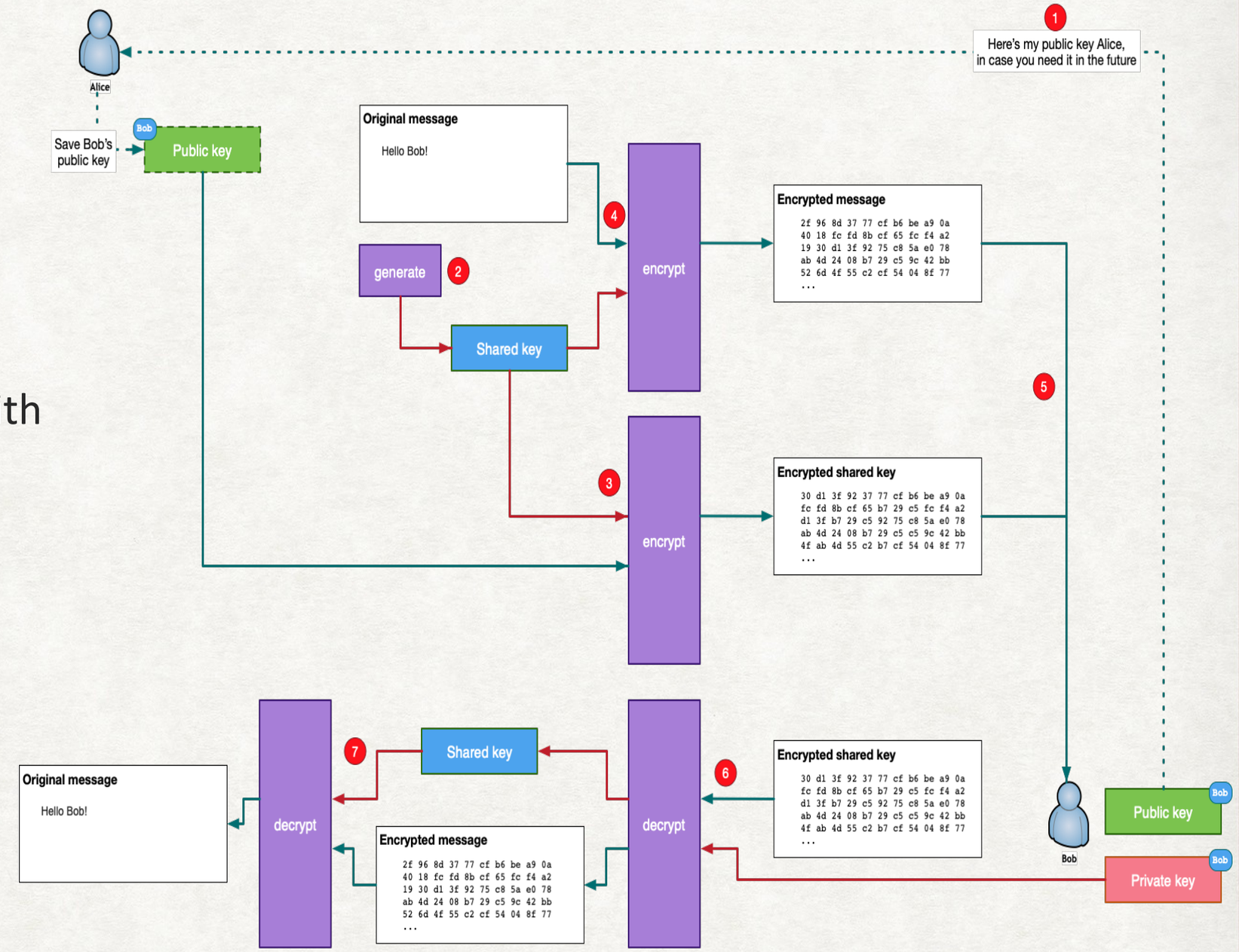
- In a symmetric encryption system such as DES, the shared key must be protected from access by others.
  - the strength of any symmetric cryptographic system rests with the key distribution technique.

- This is where asymmetric or public-key cryptography comes in handy.

- Two most commonly used public-key algorithms
  - RSA (Ron Rivest, Adi Shamir, and Len Adleman)
  - Diffie-Hellman

ASYMETRIC KEY ENCRYPTION - SECRET KEY DISTRIBUTION

1. Bob sends his public key to Alice.
2. Alice generates a shared symmetric key.
3. Alice encrypts the symmetric key with Bob's public key.
4. Alice encrypts the message with the shared key created in (2).
5. Alice sends to Bob the encrypted message and the encrypted shared key.
6. Bob decrypts the shared key using his private key.
7. Bob decrypts the encrypted message using the shared key.



https://betterprogramming.pub/an-introduction-to-public-key-cryptography-3ea0cf7bf4ba

ASSYMMETRIC ENCRYPTION (or PUBLIC-KEY ENCRYPTION)

Diffie-Hellman Protocol

- A and B are the parties that want to communicate securely. They need a **shared secret key**.

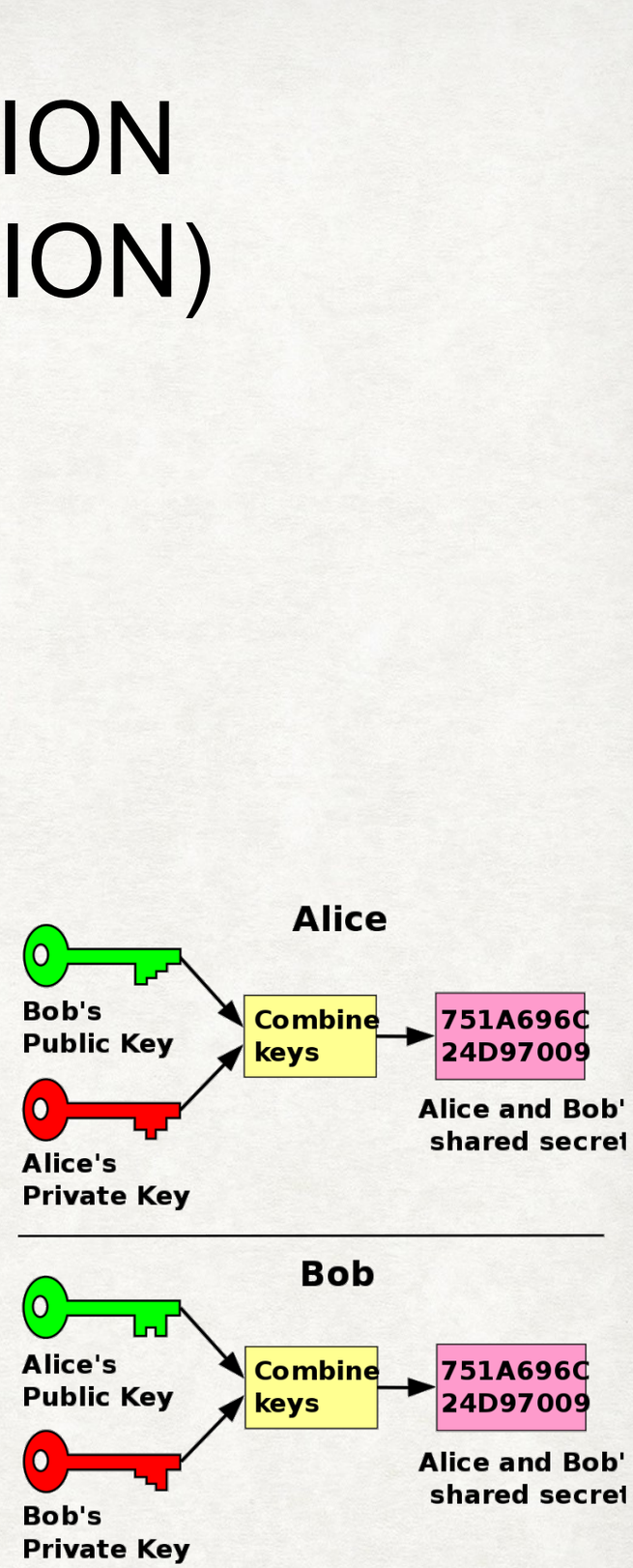
- There are two public values: one is a large prime number *p* and the other, *g*, is related to the prime number *p* (*g* primitive root modulo of p).

- Both parties generate a random private key. A produces key 'a' and B produces key 'b'.

- From these keys and the two original public values, both can produce public values they transmit to each other.

- A shared secret key can then be produced by combining the public key each gets from the other with their private keys.

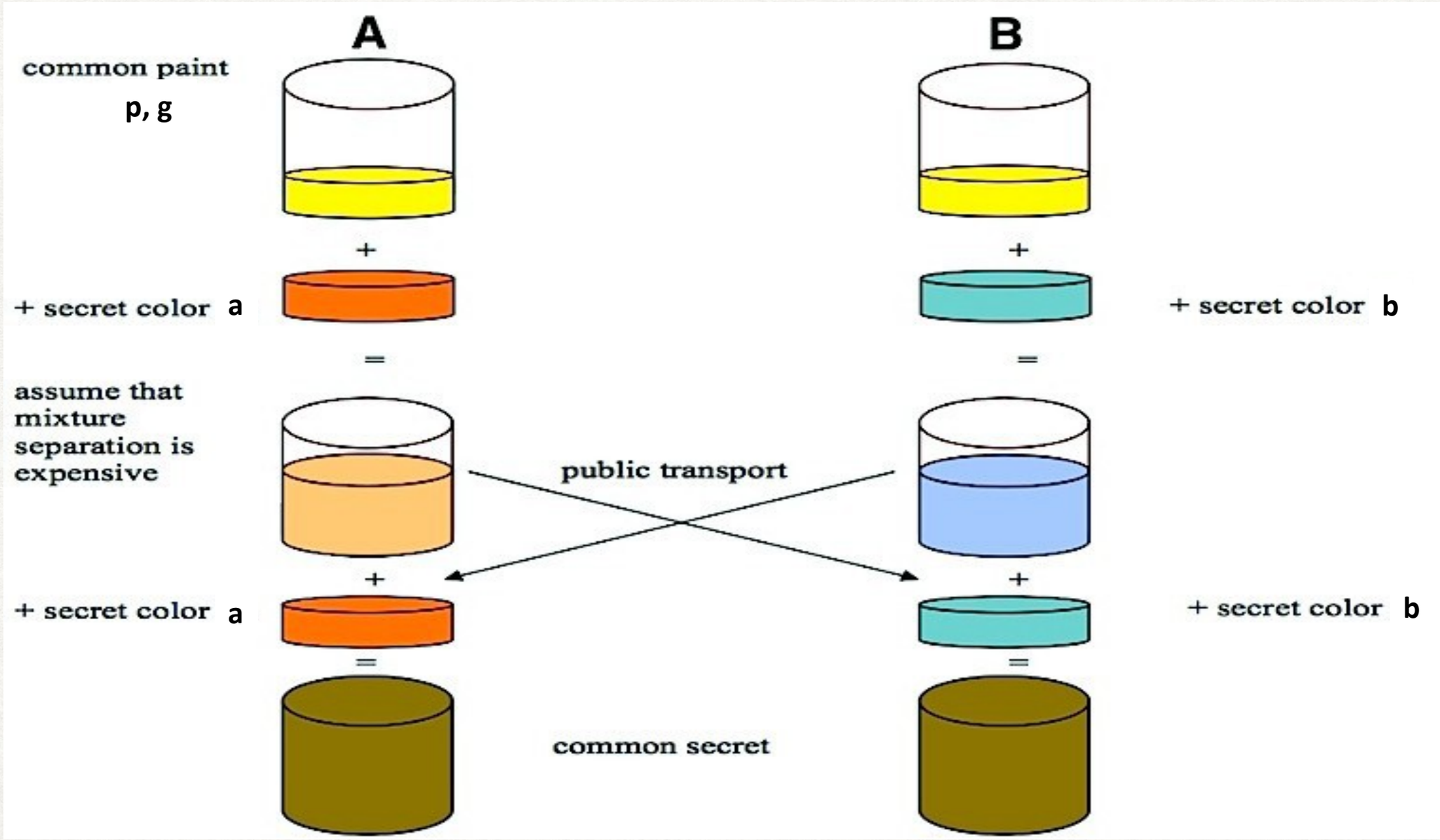
- This shared key cannot easily be broken, with the public values.



http://en.wikipedia.org/wiki/Diffie-Hellman

ASSYMMETRIC ENCRYPTION (or PUBLIC-KEY ENCRYPTION)

Diffie-Hellman Protocol



http://en.wikipedia.org/wiki/Diffie-Hellman

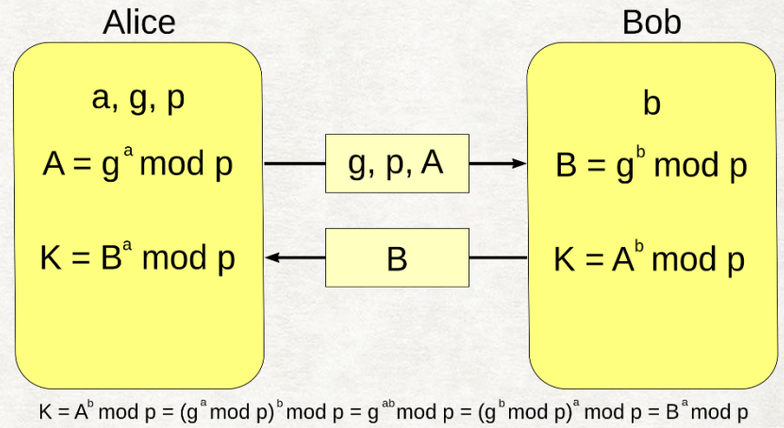
ASSYMMETRIC ENCRYPTION (or PUBLIC-KEY ENCRYPTION)

Diffie-Hellman Example

- Large prime number p = 23 (modulus), g = 5 (base).

→ *public transport = g^a mod p*

- Alice chooses secret number, a = 6.
  - Generates A = 5^6 mod 23 = 8 (sends to Bob)
- Bob chooses secret number, a = 15.
  - Generates B = 5^15 mod 23 = 19 (sends to Alice)



→ *secret key = B^a mod p (Alice) or A^a mod p (Bob)*

- Alice then generates the secret key K = 19^6 mod 23 = 2
- Bob generates the secret key K = 8^15 mod 23 = 2

- So, 2 can be used as the secret key.

- In use, p would be a huge number, about 300 digits, and the random numbers would have about 100 digits.

https://modulocalculator.com/